Understanding Saudis' privacy concerns when using WhatsApp

Understanding Saudis' privacy concerns when using WhatsApp

Yasmeen Rashidi
Indiana University
yrashidi@indiana.edu

Kami Vaniea
The University of Edinburgh
kvaniea@inf.ed.ac.uk

L. Jean Camp
Indiana University
ljcamp@indiana.edu

***Abstract*—Managing privacy in mobile instant messaging is a challenge for designers and users alike. If too many options are provided, the privacy controls can become complex to understand and unwieldy to manipulate. Conversely, providing too few controls leaves users without the ability to adequately express their privacy preferences. Further complicating this, a new class of social networks has emerged where one person can add another without mutual consent (i.e. Tumbler, Twitter, and WhatsApp). We present a survey of 626 Kingdom of Saudi Arabia (Saudi) WhatsApp users to determine their privacy-related behaviors and opinions. We find that Saudi users were aware of the privacy settings and use them especially to limit the visibility of when they were last active. We also find that 83.9% of respondents had been contacted by a stranger through the application. Respondents wanted more control over their membership in groups and the resulting visibility of their private profile information such as phone numbers. We discuss the results in terms of prior privacy and interruptibility awareness literature.**

I. Introduction

The popularity of Mobile Instant Messaging (MIM) applications has been markedly increasing in recent years as a way to cheaply stay connected with friends and family. MIM applications such as WhatsApp, Google Hangouts, Facebook Messenger, and Snapchat allow users to easily send text messages, videos, links, and photos. They also enable the maintenance of online communities through the use of group pages and multi-party chat features. However, the visibility of users' personal information to other users on these networks leads to privacy concerns. To help counter these issues, applications provide privacy features and settings that can be used to manage the visibility of information. However, these controls do not always a match to users' expectations and needs.

While the use of MIM enables easier communication, it also brings with it privacy issues inherent in Computer Mediated Communication (CMC) such as how to limit the visibility of information to intended audiences. CMC applications also suffer from privacy concerns around controlling and disseminating awareness or presence information [27]. Even though they are using MIM to communicate information to others, users still have an expectation of privacy. Prior work has found that users of CMC technologies such as WhatsApp use them to effectively collaborate with others at work [37], but still want to limit the sharing of awareness type information such as location to specific groups in specific contexts. For example, sharing location information with co-workers only during work hours while sharing the same information with spouses all the time [9], [28].

Privacy also varies depending on cultures [38]. Studies have found that culture has a huge impact on online privacy concerns [5], the pattern of use of social networks [35], and the SNS privacy policies [6]. Most cultural privacy research focuses on Western cultures, with minimal research done with Middle Eastern cultures. In this work, we are interested in how users of Kingdom of Saudi Arabia (KSA) manage their privacy in an application that provides simplified coarse grain privacy controls to users. We selected WhatsApp because the application is very popular in many countries [14], including KSA, and puts a strong emphasis on being simple and easy to use. This design philosophy has resulted in two interesting choices: 1) coarse grain control options, and 2) one-sided connections where one person can add another person as a connection without the other person's notification or approval. These features lead us to focus on the following research questions:

- R1: *How do Saudi users control access to their information using WhatsApp settings?* In particular, we are interested in users' awareness of privacy issues on WhatsApp, the privacy setting choices they make, and their opinions about the privacy options available to them.
- R2: *How do Saudi users manage issues associated with one-sided connections?* In particular, we are interested in three issues with one-sided connections: unwanted contact through the application, being added to a chat group without permission, and blocking as a way to manage one-sided connections.

We administered a survey about privacy setting usage on WhatsApp and the avalible opinions regarding WhatsApp privacy. The survey was sent to WhatsApp users in KSA using a snowball sample methodology.

We found that: 1) Setting simplicity was generally liked by respondents; however, they also wanted the ability to limit the visibility of information to specific people. 2) Respondents wanted to be asked before being added to a group. 3) Contact

USEC '16, 21 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2016.23022

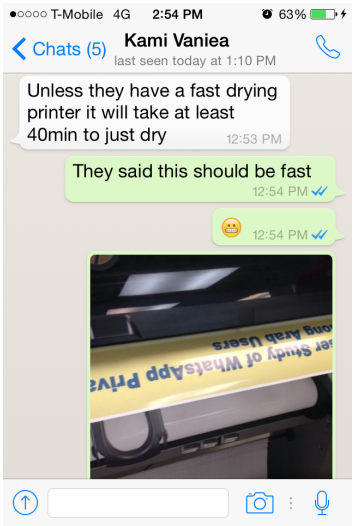

Fig. 1: WhatsApp conversation between two users (iOS version).

Fig. 2: WhatsApp Group Chat where phone numbers are shown for members who are not a part of the phone contact list and members names are shown for the members on the phone contact list.

from strangers was an issue for 83.9% of respondents. 4) Though males and females used the blocking feature to control unwanted contact from both strangers and known contacts, women tended to block strangers more often than men. We conclude with a discussion of these results and the limitation of our work.

II. WhatsApp

WhatsApp Messenger is a cross-platform mobile messaging application launched in 2009. It was initially designed as a text messaging application, but its current version allows for the creation of groups, sending media (images, audio and video), sharing of contacts details, and sharing the user's location. The current application allows communication between two or more users (Figure 1) where chat histories are recorded and visible to all parties.

WhatsApp is popular in several countries, it is an inexpensive form of communication because of the phone's ability to use free wireless access points or existing data plans to send messages, easy to use due to its simplistic interface, and ad free [8], [32].

WhatsApp is continuously altering the way privacy is managed on the application. The following describes the functionality of WhatsApp at the time of the study (November, 2014).

WhatsApp uses phone numbers to uniquely identify users. When a user first signs-up with WhatsApp, she has to provide and verify her phone number. This becomes her unique identifier on the application.

The contacts list on WhatsApp is drawn directly from the phone's contact list. After setup, WhatsApp reads the contact list on the user's phone and automatically adds all her contacts who are on WhatsApp to her WhatsApp contact list. If she wants to connect with another WhatsApp user she must add that person's phone number to her phone's contact list which automatically adds the person as a contact on WhatsApp. The only way to remove someone from WhatsApp's full list of contacts is to delete them from the phone's list of contacts.

Mutual consent is not required to add someone as a contact. If Bob adds Alice as a contact he can immediately contact her and see her profile information as soon as he has added her. Alice does not need to provide any explicit consent for this to happen and Alice cannot see that Bob has added her to his contact list.

Phone numbers are visible to all members of a Group Chat. A Group Chat is a conversation amongst a group of WhatsApp users. Each message sent to the Group Chat is sent to everyone who is a member of that chat. Anyone can create a new Group Chat and add up to 49 other users. Added users are immediately included in the group without mutual consent and notified about their new membership. The existing Group Chat members will see a message that a new member joined the group. Membership is visible to all participants. Mutual authentication is not needed to add a user, but they may leave the group at any time. Doing so will trigger a message sent to the whole group stating: "[User] left." All group members can see the phone numbers of all other group members. Communications from people not in the local phone's contact list appear as phone numbers in the Group Chat (Figure 2).

The only way to prevent communication is by blocking. Anyone with a user's phone number can contact her through WhatsApp. The only way to prevent contact is by blocking the other user. Blocking a user will prevent all future contact and hide all future edits to profile information.

Profile information is visible to all users by default. Anyone who has the user as a contact can by default view her profile information which includes the profile photo, status, and when she was last using the application (last seen). The user has the ability to limit the visibility of her profile information to "Everyone", "My Contacts", and "Nobody" (Figure 3).

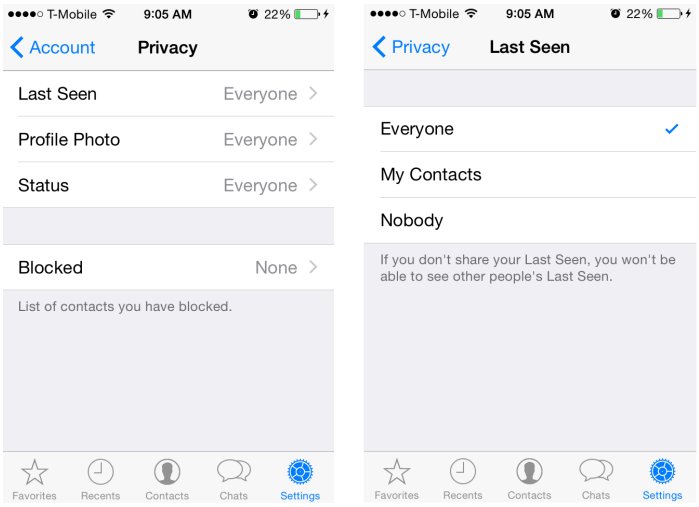

Fig. 3: WhatsApp privacy settings management interface at the time of the study (iOS version). Left: Privacy management screen. Right: Available options for Last Seen, Profile Photo, and Status.

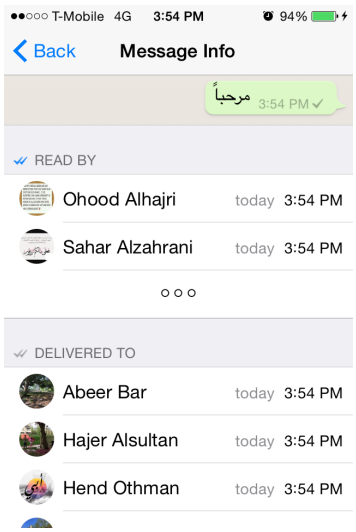

Fig. 4: WhatsApp "Read Receipts" in a Group Chat (iOS version).

Users can see when messages are delivered and read. Originally WhatsApp only provided information about message delivery to all users but three days before the study they added a feature that allows people to see when messages have been read which they refer to as "Read Receipts". As can be seen in Figure 4, the Read Receipt feature allows a user to see who has received their messages and when those messages were received and read. At the time of the study there was no way to turn this feature off.

III. Related Work

A. Managing permissions.

Ideally a user should be able to post information to an online community and be assured that her information will only be shared with those people whom she wished to share with. In practice, users can have difficulty understanding the complex permission options available to them leading them to make errors, which puts their data at risk of unintended disclosure [11], [20]. Studies on Online Social Networks (OSN) have observed a lack of awareness about privacy settings among Facebook users [1], [18]. While some users were not aware of Facebook privacy settings, others did not know where the privacy settings were located, or that they existed at all [1], [11].

People have complex ever-shifting social groups which can be challenging to track using manual grouping [19]. Additionally, many access-control management systems found in OSN require the user to construct groups of people and assign abilities to the groups.

Another study of Facebook and its privacy illustrated that groups that users were least comfortable with are not just limited to strangers, or people who are not members of the persons network, but also include other groups such as people the user has never met in person, coworkers, and friends of friends [17]. Privacy concerns have also been found to vary by gender. Studies about privacy on OSN have also noticed that women are more likely to have private profiles [22] and use privacy settings tool than men [18].

B. Privacy in Instant Messaging (IM).

IM users have three main points of privacy concern: privacy from non-contacts, privacy regarding availability, and privacy regarding the content of IM communication [27]. The majority of people are concerned about the types of information displayed to people outside their intended audience [17], [23]. Online social networks such as Facebook have endeavored to address these concerns by providing privacy controls to end users that, enabling them to control who can see what information.

Profile information such as when the person was last logged in, their current status, or current location provides information that is potentially useful to other people who might want to communicate with them. While there is a natural inclination to hide such information for privacy reasons, sharing it also enables improved coordination with other people. Patil and Lai found that office workers found sharing this type of information during work hours to be both acceptable from a privacy perspective and beneficial to work coordination [9], [28]. They also found that people were happy to share this information with their family as well, but without the work hours restrictions [28].

C. WhatsApp privacy and security.

Security and privacy have been an ongoing issue for WhatsApp with several researchers identifying security issues [10], [31]. In 2013 the Office of the Privacy Commissioner of Canada (OPC) determined that WhatsApp was breaching privacy laws [24]. Although WhatsApp worked on some of these violations (e.g. messages encryption, sharing of status messages and presence), some are still in existence.

WhatsApp was initially used to communicate with close friends and sometimes family [8]. Even more recent studies

have found that people tend to use it to communicate with tightly connected groups of people in small geographical areas [25]. WhatsApp self describes itself as using "your phones Internet connection to message and call friends and family" [15]. However, as WhatsApp becomes more popular and more ubiquitous it is being used for all sorts of purposes such as sharing medical information [37], helping students learn to read [30], and sharing documents [7].

Church and Oliveira investigated the Last Seen feature in WhatsApp. This feature allows Alice, for example, to know the last time her contact Bob opened WhatsApp. The research illustrated that the recipient feels pressure to respond, regardless of the urgency of the sender. "If I send a WhatsApp to him, I check for the 2 ticks and if I don't get a reply, then I think but he read it!" While some users see this as an invasion to their privacy "I don't like it very much because if I don't want to answer straight away, I don't want them to know that I've seen the message", others rely on the immediacy of the program "It doesn't need to be answered in that moment but I know you're going to read it" [8]. In another study using WhatsApp O'Hara et al. [25] talked about how different patterns of using awareness and notifications provided by WhatsApp (e.g. last seen and double checks) create accountabilities and raise the issue of moral implications for the application design. While some users see last seen as invitation to talk others do not see it as a notation of availability.

D. Culture and privacy

User privacy preferences and behaviors may vary depending on, for example, gender, culture, region or religion. In their research, Zakaria, Stanton, & Sarkar-Barney illustrated that cultural values play an important role in how people manage privacy issues [38]. They depended on the culture values framework developed by Halls to discuss the differences between low-context cultures (e.g. United States, Germen, and English) and high-context cultures (e.g. Arab, Indian, Spanish, and Asian) and how these differences could relate to privacy. A study for Wang et al. [36] found that American social network users have more privacy concerns than their Chinese and Indian counterparts, and what they considered as private information differs between cultures.

Culture can also have a strong impact on how men and women interact involving technology. Work on security and privacy of banking in the Kingdom of Saudi Arabia has shown that men and women have different types of expectations around the sharing of potentially private information such as banking PIN numbers [2]. Research on empowering women in developing countries through technology also highlights the need to take culture and privacy into account. Shroff and Kam recommend that applications aimed at women in developing countries be designed so the user interface evolves as the women becomes more accustomed to using the technology [33]. Women in these areas often start out unsure and unwilling to take an active participating role. As they become more accustom to interacting with the technology they become more willing to take a proactive role; the user interface needs to support this transition.

IV. Methodology

A web-based survey was used to elicit user behaviors and perceptions relating to the use of WhatsApp. The survey focused mainly on privacy issues surrounding the management of profile information and the ways people communicate using WhatsApp. Several questions in the survey also addressed attitudes and behaviors regarding unwanted communication based on how WhatsApp uses the phone number as an user ID. The survey was written in English and one of the authors, native speaker of Arabic, translated the survey into Arabic. Both versions of the survey were tested by native speakers in both languages.

A. Survey Design

The survey contained 42 questions, the majority of which were multiple choice and Likert scale questions. It was comprised of: 5 demographics questions; 5 questions about what MIMs respondents have/are using and reasons of downloading those MIMs; 6 questions about WhatsApp usage; 13 questions asking about the respondents current non-privacy settings in the app (e.g. chat backup, auto download, and read receipts) and their opinions/knowledge about them; 4 questions asking respondents about blocking features and why they have used them; 3 questions asking them if they had been contacted by stranger(s) using WhatsApp; 3 questions that asked the respondents to specify their current privacy settings in the app and why they chose these settings; 1 question which had a 5-point Likert scale that asked the respondents to indicate their degree of agreement with 19 statements about WhatsApp; and finally the last 2 questions asked the respondents about the feature(s) that they dislike the most in the current version of the app and the feature(s) that they would like to see. The end of the survey had a free text comment box. All the questions were based on how WhatsApp functioned at the time of the survey and its privacy settings. Differences between different OS platforms were taken into account.

B. Sampling Methodology

Participants who responded to the survey were recruited using a snowball sampling methodology through WhatsApp itself. Participants did not receive any compensation. The participants were informed that we are studying WhatsApp privacy settings and the work was approved by our IRB.

The first author is a citizen of the Kingdom of Saudi Arabia and was able to use her existing WhatsApp contact list to advertise the survey to Saudi users of WhatsApp. The initial seed was encouraged to share the survey with other contacts. She also posted advertisements for the survey on public social networking pages for Saudis in the United States.

C. Sample Demographics

A total of 1238 respondents accessed the online survey, and 945 respondents completed it. Most respondents identified themselves as Arab (Saudi)(74.4%, n=626), while (22.75%, n=215) were Arab, (2.43%, n=23) were Indian, (1.48%, n=14) were American, (1.27%, n=12) were Asian, and (5.92%, n=56) chose not to identify themselves. In this study we focus our analysis on the 626 respondents who completed the survey and identified themselves as Saudis. 137 (21.88%) of our

Group	Always	Often	Rarely	Never	No Answer
Family	65.2%	27.6%	6.4%	0.5%	0.3%
Friends	59.9%	29.4%	8.1%	0.5%	2.1%
Co-Workers	26.8%	30.8%	28.9%	10.1%	3.4%
Others	4.5%	7.8%	33.2%	52.1%	2.4%

TABLE I: How often respondents contact each group through WhatsApp (percentage of respondents).

respondents were aged 18-24, 290 (46.33%) were aged 25-30, 133 (21.25%) were aged 31-40, 55 (8.79%) were 41+ and 11 (1.76%) chose not to indicate an age. The majority of the respondents were women (64.54%, n=404), and about a third were men (31.79%, n=199), with (3.67%, n=23) chose not to indicate a gender. We asked the respondents about their current employment status 240 (28.54%) were graduate students, 199 (23.66%) were employed, 192 (22.83%) were undergrad students, 155 (18.43%) were not employed, and 55 (6.54%) chose not to indicate a status.

V. Results

A. WhatsApp Usage

Most respondents (93.61%, n=586) used WhatsApp on a daily basis to connect with others. Table I shows how often respondents contacted different social groups including Friends, Family, Co-workers and Others who appear on their contact list such as drivers, plumbers, and contractors. They contacted Always or Often most frequently with family (92.8%, n=581) followed by friends (89.3%, n=559). They were less consistent for co-workers reporting contact Always, Often, and Rarely with nearly equal frequencies. The Never option was also selected by 10.1% (n=63). While 16.6% (n=104) were unemployed it is likely that they may have had co-workers through volunteer work or in a past employment. People rarely contacted people in the Other group, with 52.1% (n=326) indicating that they never contacted people in this group through WhatsApp at all. These results are consistent with earlier work which found that people consider WhatsApp to be an informal form of communication best suited for contacting friends and family [8].

We asked respondents what type of information they used WhatsApp to send to their contacts. They sent text messages (88%, n=551), images (82%, n=515), links to information such as news (77%, n=480), videos (71%, n=447), contact information (58%, n=361), and their location (44%, n=278). When asked if they regularly used WhatsApp to send sensitive content 53.4% (n = 334) indicated Strongly Agree or Agree.

B. Awareness and Use of Settings

We asked respondents to report their current WhatsApp privacy settings. The majority (58.98%) of respondents had changed at least one setting. As can be seen in Table II, 46.6% decided to completely hide their last seen timestamps, and 11.7% decided to limit visibility to My Contacts. However, many users elected to leave their profile photo and status visible to either Everyone or My Contacts with only 2.4% and 3.8% completely removing the visibility of their profile photo and status respectively.

Group	Last Seen	Profile Photo	Status
Everyone	46.6%	68.0%	70.0%
My Contacts	11.7%	23.5%	19.8%
Nobody	33.0%	2.4%	3.8%
I don't have this feature	8.0%	4.3%	4.1%
No Answer	0.8%	1.8%	2.2%

TABLE II: Respondent self-reported privacy settings (percentage of respondents).

Profile Information	Agree	Neutral	Disagree	NA
Profile picture	43.3%	25.1%	30.7%	1.0%
Status	45.2%	25.0%	28.1%	1.8%
Last seen	47.3%	23.8%	27.3%	1.6%

TABLE III: Answers to: *I want to be able to hide my [profile information] from specific people in my contact list.* We grouped Strongly Agree and Agree under Agree and Strongly Disagree and Disagree under Disagree (percentage of respondents).

Based on prior work, we anticipated that respondents would consider their last seen information to be sensitive and asked why they chose to hide or not hide it. Respondents did not feel that it was necessary to hide their last seen information (44.2%, n=277). Only 4.5% (n=28) of respondents said that they were not aware of the setting, and 4.3% (n=27) said they did not think about this issue before.

WhatsApp provides coarse-grained control over who can see profile photos, statuses and last seen (Figure 3). There is no custom group setting, so users must give access to Everyone, My Contacts, or Nobody. We asked the respondents if they would like to exclude specific people from seeing their three types of profile information on a 5-point Likert scale (Table III). Respondents generally agreed that they wanted to limit specific peoples' ability to see their profile information (43.3% – 47.3%).

Using a 5-point Likert scale we also asked the respondents to indicate whether they agree or disagree that the application should ask them before adding them to a Group Chat (i.e friending request). The vast majority of participants agreed that they would like to be asked before being added to a group (80.8%, n=506 in agreement and 7.0%, n=44 against).

Respondents were very aware of privacy-related features on WhatsApp. The survey was launched a few days after the "Read Receipts" feature was added for all platforms with no way to turn it off. This feature allows the user to know who and when others have received their message(s) and have read or played it (e.g. voice message) (Figure 4). When we asked respondents about this update, 95.8% (n=600) of them indicated that they were aware of the feature. When we asked respondents if they had used the read receipts feature or not, 17.7% (n=111) of users said that they had used it to check who had read their messages and when, while 48.9% (n=306) said that they only sometimes use it.

C. Managing Unwanted Contact

The majority of respondents had been contacted by strangers previously, with 66.6% (n=417) having been con-

Reason	Women	Men
He has my number but I don't know this person	52.2%	21.6%
I have this person's phone number, but I don't want him to contact me over WhatsApp	7.2%	10.6%
I don't want him to be able to see my profile photo and/or status	9.7%	7.0%
We are not friends anymore	4.2%	8.5%
We had a bad fight	12.9%	20.1%
No Answer	13.9%	32.2%

TABLE IV: Reasons why men and women who have blocked someone before chose to block people. Values shown as a percentage of women and men due to the uneven number of female versus male respondents.

tacted more than once, 17.3% (n=108) saying they were contacted once, and 14.2% (n=89) reporting to have never been contacted by a stranger. We found no statistically significant difference between men and women in the frequency of contact by strangers. The majority of respondents 337 (53.8%) agreed that it bothers them that a stranger can see their profile information while 179 (28.6%) said "maybe".

The only available way to prevent future contact from another user is by using the blocking feature. The majority of the respondents (75.1%, n=470) reported having used the blocking feature in the past. Women (81.7% of female respondents) were statistically more likely to use the blocking feature than men (62.8% of male respondents) (χ^2 test value of 337.57, df = 1, $p =< 0.00001$, controlled by removing respondents who were not aware of the feature or chose not to answer). We asked respondents to select the most common reason they block others on WhatsApp from the list of the potential reasons shown in Table IV. We found that men and women's reasons for blocking were statistically significantly different (χ^2 test value of 788.13, df = 4, $p =< 0.00001$, controlled by removing respondents who chose not to answer). Both genders tended to block because the other person was a stranger, or because they had had a fight with the person, but woman were more likely to block strangers, and men were more likely to block after fights.

VI. Discussion

A. Controlling access to profile information

Early research on doing collaborative work using Instant Messaging applications focused on providing awareness information to contacts so that collaborators could select a communication time when the person was not busy [26]. Systems were created that could help provide availability information by determining contact's availability based on prior communication patterns [29], and automatically determining how interpretable the person was and broadcasting that information to others [13]. However, potential communicators tended to not limit communications based on interruptibility, instead they used the awareness information only to determine if the other person was present and likely to respond [13]. Understandably users developed privacy sensitivity to the awareness information being shared [28].

WhatsApp provides users with two types of awareness information: when the user was last seen using the application, and if they have read a message. Our respondents were more sensitive about sharing last seen information with others than they were with other profile information, such as profile photo and status. In this study we only asked about the last seen information because the feature providing information about when users read messages had just been released in an update and was only available to some users. This result is consistent with prior literature studying the concerns of WhatsApp users, which found that users have privacy concerns about making their availability known [8], [25]. What was particularly interesting in our results was that while privacy settings for all the profile information is co-located on the same screen, many participants chose to only restrict the visibility of the last seen information, suggesting that they view last seen as more privacy concerning than profile photo or status information.

WhatsApp's all-or-nothing style of permissions settings gives users a very coarse grain control over the size and composition of the audience for their profile information. People tend to have multiple facets to their interactions. For some people those facets are highly overlapping, and for others the facets are disjoint [12]. The simple permission design makes the application easy to use, and it provides good support for people who have highly overlapping facets, or people where only members from one facet use WhatsApp. It does not well support users who have minimally overlapping or disjoint facets. To help handle this issue other Online Social Networks, such as Facebook, provide users with the ability to create custom groups or add contacts to a pre-defined "limited access" group. Even adding two simple choices (e.g. Always Share With and Never Share With) that override the current settings list provides users with the ability to make exceptions to their settings [34].

B. One-sided connections

WhatsApp was initially designed to help people communicate informally with friends and family. Many of the privacy management choices reflect this starting point of view. The choice to use the phone number as the only information needed to connect assumes that only people the user knows well would have her phone number. Similarly the choice to use a one-sided handshake to add a new contact is an example of privacy through obscurity; access to profile information is naturally limited as long as only people that the user knows have access to her phone number. As long as the obscurity assumption holds, the user gets good enough privacy and an application that is easy to set up.

Part of the problem with using the phone number as the sole requirement for forming a connection is that phone numbers are not necessarily as private as they are assumed to be. WhatsApp itself supports a group chat feature where chat members can see each others phone numbers. Similar to the obscurity assumptions mentioned above, as long as Group Chat is used for a small number of known contacts the visibility of phone numbers is not an issue. The problem is that as WhatsApp is becoming more popular, it is starting to be used for new purposes. What was once a communication channel limited to friends and family, started to be used for communication in other contexts [28], [30], [37] where people who do not know each other may end up on the same Group Chat. Additionally, users sometimes share their own and others phone contact

information publicly through online social media [16]. In our own study 53% of respondents used WhatsApp to send contact information to others. The information sharing in Group Chat allows people who are either strangers or who have only a passing relationship with the user to get her phone number and start contacting her. Our respondents wanted more control over membership in Group Chats.

Unwanted contact by strangers was a common experience for our respondents with 83.9% of them being contacted by a stranger. We found that Saudi women were more likely than men to use the blocking feature after being contacted by a stranger. This might due to the nature of relationship between men and women in KSA. The Quran[1] warns against mixing between different sexes which could lead to "seduction and the 'evil consequences' that might follow" [3]. Culturally, gender separation is an implicit rule in public and private life activities in KSA [4]. It is normal for women and men to remain physically separated unless they are in public or with family. Due to this, men have less opportunities to communicate with women outside their own families. WhatsApp may seem like a safe way to approach and communicate with women without publicly breaking the religious and tradition rules.

Managing unwanted communications from either strangers or known contacts puts a burden on users who have to block each unwanted contact individually. Unwanted communications invade users' privacy and potentially put them at risk of stalkers who may simply keep contacting them using different phone numbers. The only choice is to individually block unwanted users' phone numbers, which does not prevent future new unwanted contacts. A female respondent explained in the comment section that:

> *"I once I had to delete my phone number because of a stalker that kept sending me messages from different phone numbers. Blocking his numbers was not effective. That was a breach of my privacy."*

The ability to limit communication to only an approved list of contacts would assist users like this one. However, it might also put a privacy configuration burden on users who may not need the functionality making WhatsApp less user friendly.

While unwanted contact is primarily annoying, it can also be dangerous for users. Strangers can send media files, links, and even viruses that users might open allowing the stranger to learn information about the user's location or even install software that lets them spy on the user. Almost half of our respondents downloaded and opened media sent to them by people that they did not know or were not sure about their identities (8.5% Always, 40.3% Sometimes). Spam is also becoming an issue on WhatsApp, enough so that a recent update added a "report spam" button to flag and remove spam related to unwanted contact from the system.

The ability to add people to groups without mutual consent combined with the automated notification of the whole group on exit causes social pressure to remain in groups. One of the key privacy concerns in social networks and instant messaging application is reputation management [21]. Users cannot control which groups they are added to and if they do not want to be in a group their only options are to: 1) leave the group which causes a notification to be sent to the whole group, or 2) remain in the group and ignore all the messages. Taking the first option may lead to social consequences as other group members may be upset about the user leaving the group. Taking the second option means that the user's phone number and other profile information remains visible to all group members.

[1]The central religious text of Islam.

VII. Limitation

This work makes use of a snowball sampling methodology which, while powerful, has several important limitations. The participants in this survey are likely to have a higher inter-connectivity than would be seen in the general population. Participants were also able to easily self-select in or out of taking the survey, leading to a sample of people who are inclined to take surveys on WhatsApp. One positive side effect of the snowball sampling inter-connectivity is that respondents likely received the survey URL from a friend or someone they knew. This allowed us to draw from a sample of people who might normally ignore requests from strangers.

The survey results also rely on self-reported settings and behaviors. People who misunderstand their current settings may respond based on their understanding and not look at what their settings actually are. People may also either misremember events or choose to respond based on what they know they should have been doing.

Finally, because the survey was primarily advertised on WhatsApp, our results are limited to people who are still using the WhatsApp application. People with strong privacy concerns regarding WhatsApp may have stopped using the application, effectively removing them from our sample pool.

VIII. Conclusion

Our survey contributes to the body of literature on how users manage their privacy using MIM applications. We conducted this survey to understand how Saudi users manage their privacy using the coarse settings in WhatsApp as well as how they manage issues of one-sided connections.

Our work shows that Saudi users are aware of the privacy settings, and make use of them. While some users liked the current setting options, others want the ability to limit the visibility of profile information to specific people in their contact list. The majority of users want to be asked before they are added publicly to social groups such as Group Chat.

Users use the blocking feature to control access to their profile information or control others' ability to contact them using the application. We find that women and men receive unwanted contact by strangers. However, women tend to block unwanted contact from strangers more than men.

People are developing a greater dependence on MIM applications as their primary communication mechanism. Privacy is therefore an important component that should be considered by the developers of such applications. WhatsApp emphasizes ease of contact and sharing content which which is good for usability and adoption. But the simplicity can also make it challenging for users to do fine grain management of their privacy. MIM designers need to be aware that users need

privacy tools that empower them to control their privacy in a way that matches their context.

REFERENCES

[1] Alessandro Acquisti and Ralph Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies*, pages 36–58, 2006.

[2] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. Security practices for households bank customers in the Kingdom of Saudi Arabia. In *Symposium on Usable Privacy and Security*, 2015.

[3] Mona Almunajjed. *Women in Saudi Arabia Today*. Palgrave Macmillan, 1997 edition edition, 1997.

[4] Roula Baki. Gender-segregated education in saudi arabia: Its impact on social norms and the saudi labor market. *Education policy analysis archives*, 12(28):n28, 2004.

[5] Steven Bellman, Eric J Johnson, Stephen J Kobrin, and Gerald L Lohse. International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5):313–324, 2004.

[6] Joseph Bonneau and Sören Preibusch. The privacy jungle: On the market for data protection in social networks. In *Economics of information security and privacy*, pages 121–167. Springer, 2010.

[7] Patient Rambe1 Crispen Chipunza. Using mobile devices to leverage student access to collaboratively-generated resources: A case of WhatsApp instant messaging at a South African university. In *International Conference on Advanced Information and Communication Technology for Education*, 2013.

[8] Karen Church and Rodrigo de Oliveira. What's up with WhatsApp?: Comparing mobile instant messaging behaviors with traditional SMS. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, pages 352–361, 2013.

[9] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, Portland, Oregon, USA, April 2-7 2005.

[10] Scott Coull and Kevin Dyer. Privacy failures in encrypted messaging services: Apple imessage and beyond. Technical report, 2014.

[11] Serge Egelman, Andrew Oates, and Shiriram Krishnamurthi. Oops, I did it again: Mitigating repeated access control errors on Facebook. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, 2011.

[12] Shelly D. Farnham and Elizabeth F. Churchill. Faceted identity, faceted lives: Social and technical issues with being yourself online. In *Proceedings of Computer Supported Collaborative Work*, 2011.

[13] James Fogarty, Jennifer Lai, and Jim Christensen. Presence versus availability: The design and evaluation of a context-aware communication client. *International Journal of Human-Computer Studies*, 2003.

[14] GlobalWebIndex. Share of mobile internet users in selected countries who are active whatsapp users as of 4th quarter 2014, 2014. http://www.statista.com/statistics/291540/mobile-internet-user-whatsapp/. (Last accessed 1-12-2015).

[15] WhatsApp Inc. WhatsApp Messenger. https://play.google.com/store/apps/details?id=com.whatsapp. (Last accessed 1-20-2015).

[16] Prachi Jain, Paridhi Jain, and Ponnurangam Kumaraguru. Call me maybe: Understanding nature and risks of sharing mobile numbers on online social networks. In *Proceedings of the First ACM Conference on Online Social Networks*, COSN '13, pages 101–106, New York, NY, USA, 2013. ACM.

[17] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. Facebook and privacy: it's complicated. In *Proceedings of the 8th Symposium on Usable Privacy and Security*, 2012.

[18] Harvey Jones and José Hiram Soltren. Facebook: Threats to privacy. *Project MAC: MIT Project on Mathematics and Computing*, 1:1–76, 2005.

[19] Patrick Gage Kelley, Robin Brewer, Yael Mayer, Lorrie Faith Cranor, and Norman Sadeh. An investigation into Facebook friend grouping. In *Proceedings of 13th IFIP TC13 Conference on Human-Computer Interaction*, pages 216–233, 2011.

[20] Jennifer King, Airi Lampinen, and Alex Smolen. Privacy: Is there an app for that? In *Symposium on Usable Privacy and Security*, 2011.

[21] Alfred Kobsa, Sameer Patil, and Bertolt Meyer. Privacy in instant messaging: An impression management model. In *Behaviour & Information Technology*, pages 355–370, 2012.

[22] Kevin Lewis, Jason Kaufman, and Nicholas Christakis. The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1):79–100, 2008.

[23] Heather Richter Lipford, Andrew Besmer, and Jason Watson. Understanding privacy settings in Facebook with an audience view. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, 2008.

[24] Office of the Privacy Commissioner of Canada. Report of findings investigation into the personal information handling practices of WhatsApp inc., Jan 2013. https://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp. (Last accessed 1-12-2015).

[25] Kenton P. O'Hara, Michael Massimi, Richard Harper, Simon Rubens, and Jessica Morris. Everyday dwelling with WhatsApp. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 1131–1143, New York, NY, USA, 2014. ACM.

[26] Sameer Patil and Alfred Kobsa. The challenges in preserving privacy in awareness systems. In *Institute of Software Research, University of California*, 2003.

[27] Sameer Patil and Alfred Kobsa. Instant messaging and privacy. In *Proceedings of HCI '04*, pages 85–88, 2004.

[28] Sameer Patil and Jennifer Lai. Who gets to know what when: Configuring privacy permissions in an awareness application. In *Proceedings of the SIGCHI '05 conference on Human factors in computing systems*, pages 101–110, New York, NY, USA, 2005. ACM.

[29] Martin Pielot, Rodrigo de Oliveira, Haewoon Kwak, and Nuria Oliver. Didn't you see my message?: Predicting attentiveness to mobile instant messages. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 3319–3328, New York, NY, USA, 2014. ACM.

[30] Mar Gutiérrez-Colon Plana, María Isabel Gibert Escofet, Idoia Triana Figueras, Ana Gimeno, Christine Appel, and Joseph Hopkins. Improving learners' reading skills through instant short messages: A sample study using WhatsApp. pages 80–84, 2013.

[31] Sebastian Schrittwieser, Peter Frühwirt, Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Markus Huber, and Edgar R Weippl. Guess who's texting you? evaluating the security of smartphone messaging applications. In *Proceedings of the 19th Annual Symposium on Network and Distributed System Security*, 2012.

[32] Richard Shambare. The adoption of WhatsApp: Breaking the vicious cycle of technological poverty in south africa. *Journal of Economics & Behavioral Studies*, 6(7), 2014.

[33] Geeta Shroff and Matthew Kam. Towards a design model for women's empowerment in the developing world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2867–2876, 2011.

[34] The Telegram Team. Hiding last seen time - done right, November 2014. https://telegram.org/blog/privacy-revolution. (Last accessed 1-20-2015).

[35] Asimina Vasalou, Adam N Joinson, and Delphine Courvoisier. Cultural differences, experience with social networks and the nature of "true commitment" in Facebook. *International Journal of Human-Computer Studies*, 68(10):719–728, 2010.

[36] Yang Wang, Gregory Norice, and Lorrie Faith Cranor. Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites. In *Trust and trustworthy computing*, pages 146–153. Springer, 2011.

[37] Shabeer Ahmad Wani, Sari M. Rabah, Sara AlFadil, Nancy Dewanjee, and Yahya Najmi. Efficacy of communication amongst staff members at plastic and reconstructive surgery section using smartphone and mobile WhatsApp. *Indian Journal of Plastic Surgery*, 46:502–505, 2013.

[38] Norhayati Zakaria, Jeffrey M. Stanton, and Shreya T.M. Sarkar-Barney. Designing and implementing culturally-sensitive IT applications: The interaction of culture values and privacy issues in the middle east. *Information Technology & People*, 16(1):49 – 75, 2003.